

Abstract of CH 675 920 A

In a method of protecting a device against unintended use a token T serves as an electronic key and is embodied as a chip card 20 with an internal memory comprising several storage locations 8. The electronic key is adapted to cooperate with a device part S comprising an internal memory 2, a random number generator 3, an encryption unit 4, a comparing unit 5 and a control unit 1. A common secret key is stored in the internal memories of the token T and device part S, respectively. The random number generator 3 generates a random number which is transferred to the token T. After that the random number in the device part S and token T is encrypted with the secret key stored in the internal memories 2 and 8, respectively. The encrypted random number generated in the token T is transferred to the device part S and compared in the comparing unit 5. If the comparison is positive, the comparing unit 5 controls the control unit 1 so as to execute the desired application.



SCHWEIZERISCHE EIDGENOSSENSCHAFT
BUNDESAMT FÜR GEISTIGES EIGENTUM

⑪ **CH 675920 A5**

⑤① Int. Cl.⁵: **G 07 C** 9/00
E 05 B 49/00

Erfindungspatent für die Schweiz und Liechtenstein
Schweizerisch-liechtensteinischer Patentschutzvertrag vom 22. Dezember 1978

⑫ **PATENTSCHRIFT** A5

⑳ **Gesuchsnummer:** 1937/88

㉔ **Anmeldungsdatum:** 20.05.1988

㉔ **Patent erteilt:** 15.11.1990

㉔ **Patentschrift veröffentlicht:** 15.11.1990

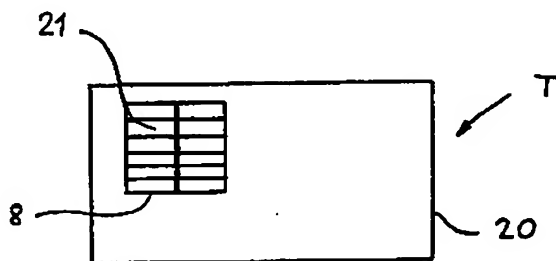
㉔ **Inhaber:**
Gretag Aktiengesellschaft, Regensdorf

㉔ **Erfinder:**
Schöbl, Paul Jakob, Dr., Zürich

㉔ **Vertreter:**
CIBA-GEIGY AG, Basel

㉔ **Zutrittskontrollverfahren und Vorrichtung zur Durchführung des Verfahrens.**

㉔ Ein elektronisches Zutrittskontrollverfahren für Geräte, welche erst nach Identifikation des Benutzers die Durchführung gewisser geschützter Operationen, bzw. den Zutritt zu geschützten Dateien ermöglichen, ermöglicht die Erzeugung von bis zu n verschiedenen Zutritts-Tokens (T). Ein Token (T) kann für bis zu n verschiedene Geräte als Zutritts-Token benutzt werden. Der Besitzer eines gültigen Tokens (T) kann weitere gültige Tokens erzeugen. Für jedes Gerät/Token Paar wird ein eigener Schlüssel erzeugt.



Beschreibung

Die Erfindung betrifft ein Zutrittskontrollverfahren für Geräte, welche erst nach Identifikation des Benutzers die Durchführung gewisser geschützter Operationen, bzw. den Zutritt zu geschützten Daten ermöglichen und eine Vorrichtung zur Durchführung des Verfahrens.

In der modernen Datenverwaltung und der Datenübermittlung besteht sehr oft das Bedürfnis und/oder die Notwendigkeit, den Zutritt zu bestimmten Dateien und Daten bzw. den Zugriff auf bestimmte Funktionen des Gerätes auf einen bestimmten Anwenderkreis zu beschränken. Insbesondere im Bereich der Sicherheitstechnik (z.B. Chiffriergeräte) stellt sich häufig das Problem, dass Geräte bzw. Apparate installiert sind, welche zwei oder mehrere Klassen von Manipulationen erfordern: einerseits sind Operationen nötig, welche vom sicherheitstechnischen Standpunkt aus gesehen unkritisch sind, wie z.B. die Überwachung und Kontrolle des Zustandes der Datenleitungen, andererseits muss auch die Möglichkeit gegeben sein, sensitive Operationen, wie z.B. das Umschalten vom Chiffrierbetrieb auf Klartextbetrieb, durchzuführen, also Operationen, deren Durchführung bzw. Aktivierung verständlicherweise nur einem begrenzten Anwenderkreis nach Identifikation des Benutzers zugänglich sein soll.

Es existieren viele verschiedene Möglichkeiten, eine solche Identifikation durchzuführen. Die klassische Methode besteht in der Verriegelung der entsprechenden Funktion durch ein mechanisches Schloss. Ein Benutzer identifiziert sich dann durch den Besitz des dazugehörigen Schlüssels. Der Nachteil dieses klassischen Zutrittskontrollsystems aus Schlüssel und mechanischem Schloss besteht in der einfachen Reproduzierbarkeit von Schlüsseln, wodurch auch nichtautorisierte Benutzer Zutritt zu geschützt geglaubten Bereichen des Gerätes erlangen können. Darüber hinaus kommt es oft auch vor, dass ein Benutzer oft mehrere verschiedene derartige oder ähnliche Geräte bedienen muss, was im Falle des mechanischen Schlosses mit zugehörigen Schlüsseln dazu führt, dass der Benutzer immer eine Vielzahl verschiedener Schlüsseln bei sich tragen muss, was wiederum ein beträchtliches zusätzliches Sicherheitsrisiko beinhaltet. Der Ausweg, einen Hauptschlüssel zu verwenden, ist nicht praktikabel, da oft mehrere Benutzer verschiedene Teilmengen einer Menge von Geräten gemeinsam benutzen, bzw. verschiedene Klassen von Zutrittsberechtigungen für gleiche Geräte besitzen.

Neuerdings kommen oft auch elektronische Zutrittskontrollsysteme zum Einsatz, in welchen der elektronische Schlüssel als sogenanntes Token ausgebildet ist. Es handelt sich dabei um ein kleines, mobiles, portables elektronisches Gerät, welches gewisse Funktionen eines Kleinrechners übernehmen kann. Ein solches Token kann z.B. als Chipkarte realisiert sein. Die Identifikation des Benutzers eines derartigen Token erfolgt auf Basis von geheimen Chiffrierschlüsseln, welche im Gerät und im Token implementiert sein müssen. Derartige bekannte elektronische Zutrittskontrollsysteme weisen die gleichen Nachteile auf, wie die bekannten klassischen.

Zusätzlich besteht die Gefahr, dass bei der Einstellung weiterer Tokens für Zutrittsberechtigungen neuer Personen, durch Umkopieren von geheimen Chiffrierschlüsseln auf diese Token diese Chiffrierschlüssel auch nichtautorisierten Personen bekannt werden können.

Es besteht daher die Aufgabe, ein Zutrittskontrollverfahren zu schaffen, welches in einfacher und sicherheitstechnisch verlässlicher Weise zwei Aufgaben erfüllt: Einerseits soll einem begrenzten Personenkreis der Zutritt zu einem Gerät, bzw. zu verschiedenen Funktionen eines Gerätes ermöglicht werden. Andererseits soll ein Token Zutritt zu mehreren Geräten verschaffen. Das Verfahren soll es erlauben, auf einfache (ohne Umweg über eine Zentrale) und sicherheitstechnisch unbedenkliche Art zusätzliche Zutrittsberechtigungen entweder einer Person auf weitere Geräte auszudehnen oder einer neuen Person zu bestehenden Geräten zu schaffen. Darüber hinaus soll für jedes Gerät-Token-System nur ein einziger geheimer Chiffrierschlüssel existieren.

Diese Aufgabe wird durch ein erfindungsgemässes Verfahren, welches im Kennzeichen des Patentanspruches 1 beschrieben ist, gelöst.

Die zweite Aufgabe, eine Vorrichtung zur Durchführung des erfindungsgemässen Verfahrens zu schaffen, wird durch eine Vorrichtung gemäss Kennzeichen des Patentanspruches 2 gelöst.

Im folgenden wird eine beispielsweise Ausführungsform der Erfindung anhand der Zeichnungen näher erläutert. Es zeigen:

- Fig. 1 eine symbolische Darstellung eines beispielsweise als Chipkarte ausgebildeten Tokens,
- Fig. 2 den Teil des einem Token zugeordneten Gerätes, welcher die Identifizierungsfunktionen durchführt mit schematischer Blockdarstellung seiner internen Funktionen.
- Fig. 3 eine schematische Blockdarstellung des Tokens und seiner internen Funktionen.

Das beispielsweise betrachtete Zutrittskontrollsystem besteht einerseits aus einem oder mehreren Geräten mit als Schloss dienenden Teilbereichen S des Gerätes, durch welches gewisse Funktionen des (der) Geräte(s) vor nicht autorisierten Benutzern geschützt werden sollen. Andererseits stehen zur Benutzeridentifikation ein oder mehrere als Schlüssel dienende Tokens T zur Verfügung.

In Fig. 1 ist ein Token T dargestellt, welches als Chipkarte 20 mit einer mehreren Speicherplätze 8 umfassenden Rechen- und Speichereinheit ausgebildet ist.

Fig. 2 zeigt schematisch den als Schloss dienenden Widerpart S zu dem Token zugeordneten Gerät mit schematischer Blockdarstellung der internen Funktionseinheiten dieses Geräteteils S.

Er umfasst einen Permanentpeicher 2, einen Zufallsgenerator 3, einen Chiffrierblock 4 und eine Vergleichseinheit 5. Übergeordnet über die zentralen Funktionseinheiten wacht und steuert eine Kontrolleinheit 1. Zusätzlich ist dieser Teil S des Gerätes mit einem Interface 6 ausgestattet, welches als Andock-port und Schnittstelle für das zugeordnete Token T dient.

Fig. 3 zeigt schematisch das Token T und seine wichtigsten Funktionsblöcke. Es umfasst in Entsprechung zu seinem Widerpart S aus zugeordnetem Gerät eine Speichereinheit 8 und einen Chiffrierblock 10, welche von einer Token-Kontrolleinheit 9 gesteuert und überwacht werden. Als Kommunikationschnittstelle dient ein Interface 7, über welches Informationen an den zugeordneten Geräteteil S übermittelt bzw. von diesem empfangen werden können.

Die Zutrittskontrolle in dem hier betrachteten System geschieht grundsätzlich nach dem bekannten «challenged response»-Prinzip, dessen Schema durch Pfeile in Fig. 2 und 3 angedeutet ist. Die Kontrolleinheiten 1, 9 stehen in Wechselwirkung mit allen jeweils zugeordneten Funktionsblöcken. Aus Gründen einer besseren Übersichtlichkeit wurde darauf verzichtet, diese Wechselwirkung in den Fig. durch Pfeile anzudeuten.

Teil S des Gerätes und Token T verfügen über gemeinsame Geheimschlüssel in ihren (nichtflüchtigen) jeweiligen Speichern 2 bzw. 8. Zuerst wird im Teil S des Gerätes in einem Zufallsgenerator 3 ein Zufalls muster erzeugt, welches über die Schnittstellen 6 und 7 an das Token T gesendet wird. Anschließend wird das Zufalls muster in Gerät und Token in einem Chiffrier-Block 4 bzw. 10 unter der Steuerung durch den aus den Speichern 2 bzw. 8 bezogenen Schlüssel chiffriert. Das im Token T erzeugte Resultat wird über das Interface 7 bzw. 6 an das Gerät gesendet. Im Gerät geschieht ein Vergleich (Block 5). Ist der Vergleich positiv, so steuert der Vergleichsblock (5) den Kontroll-Mechanismus (1) des Gerätes, so dass die gewünschte Funktion ausgeführt wird. Die gesamten Funktionsabläufe werden in Gerät bzw. Token durch die Kontrolleinheiten 1 bzw. 9 gesteuert.

Die Funktionsfähigkeit des Tokens T und auch der Geräteteile S kann im Sinne einer weiteren Erhöhung der Sicherheit von einem einzugebenden Codewort (PIN für Personal Identification Number) abhängig gemacht werden. Dieser Mechanismus ist aus Gründen der Übersichtlichkeit in den Blockschaubildern von Fig. 2 und 3 nicht eingezeichnet.

In Gerät S und Token T wird eine Menge von n (z.B. n=16) Schlüsseln für die Zutrittskontrolle definiert. Jeder dieser Schlüssel ist durch einen Identifikator (KID für Key Identifier) bezeichnet. Für jede Kombination Token T, Gerät S wird ein eigener Schlüssel erzeugt und in beiden Systemteilen auf korrespondierenden Speicherplätzen in Tabellenform abgelegt. Diese Tabelle ordnet insbesondere jedem KID den Inhalt des Schlüssels (z.B. 64 Bit) und eine Flagge, welche die Gültigkeit bezeichnet («Present Flag») enthält. Der Zustand solcher Tabellen kann nach einigen Operationen z.B. wie folgt aussehen:

Schlüsselstabelle im Gerät 1			Schlüsselstabelle im Gerät 2		
KID	Inhalt	Present-flag	KID	Inhalt	Present-flag
1	not present	1	not present
2	not present	2	not present
.			.		
.			.		
5	abcd	present	.		
.			.		
.			7	igkl	present
.			.		
.			.		
n	not present	10	efgh	present
			.		
			n	not present

Schlüsseltablette im Token A:			Schlüsseltablette im Token B:		
KID	Inhalt	Present flag	KID	Inhalt	Present flag
1	not present	1	not present
2	not present	2	not present
.			.		
5	abcd	present	.		
.			.		
7	ijkl	present	10	efgh	present
.			.		
n	not present	n	not present

Bei einem neuen Gerät ist die Funktion, welche die Erzeugung eines Tokens T erlaubt, nicht sicherheitssensitiv, d.h. sie kann ohne Identifikation durchgeführt werden. Nach der Erzeugung des ersten Tokens wird die Funktion als sicherheitssensitiv betrachtet, d.h. sie kann nur nach einer Identifikation mit einem früher erzeugten Token T ausgeführt werden.

Bei der Erzeugung von neuen Zutritts-Token T stellt sich das Problem der Bestimmung des für das neue Token T zu verwendenden Schlüssels bzw. seines KID's. Dieser KID wird nach folgendem Algorithmus bestimmt:

– Wähle den ersten KID in der Menge (1..n), so dass kein entsprechender Schlüssel im Gerät oder im Token «present» ist (d.h. dass der entsprechende Platz in Gerät und Token frei ist).

– Ist dies nicht möglich, so wähle den ersten KID in der Menge (1..n), so dass im Token der entsprechende Schlüssel nicht «present» ist (d.h. dass der entsprechende Platz im Token frei ist).

Ist dies nicht möglich, so erzeuge eine Fehlermeldung, welche besagt, dass das Token schon maximal ausgenutzt ist.

Ist ein solcher KID gefunden worden, so wird im Geräteteil S ein Zufallsmuster erzeugt und unter diesem KID in Geräteteil S und Token T abgespeichert.

Der Ablauf der Zutrittskontrolle wird im folgenden beschrieben. Nach Verbinden von Geräteteil S und Token T über die Interfaces 6 und 7 erfolgt einfach eine Suche durch die Menge der KID (1..n) nach einem Wert, so dass

– ein entsprechender Schlüssel in Gerät und Token «present» ist und

– ein Challenged Response - Verfahren gemäss «State of Art» einen gültigen Vergleichswert liefert.

Hat dieses Verfahren Erfolg, so wird Zutritt gewährt, andernfalls nicht.

Im vorstehend genannten Beispiel ermöglicht Token A den Zutritt zu Gerät 1, Schlüssel abcd auf KID 5 stimmt überein, und zu Gerät 2, Schlüssel ijkl auf KID 7 stimmt überein. Token B hingegen erlaubt nur den Zutritt zu Gerät 2, Schlüssel efgh auf KID 10 stimmt überein, welches aber auch dem Benutzer des Token A Zutritt gewährt, Schlüssel ijkl auf KID 7 stimmt überein.

Dieses neue Zutrittskontrollsystem zusammen mit dem erfindungsgemässen Verfahren zur Erzeugung von Token T, d.h. zur Generierung von Zutrittsberechtigungen, sowie der neuartige Ablauf der Zutrittskontrolle eines Benutzers weist viele Vorteile gegenüber dem Bekannten auf.

Für ein Gerät können ohne zentrale Verwaltung bis zu n verschiedene Zutritts-Tokens erzeugt werden.

Ein Token kann ohne zentrale Verwaltung für bis zu n verschiedene Geräte als Zutritts-Token verwendet werden.

Der Besitzer eines gültigen Tokens kann weitere gültige Tokens erzeugen.

Die Geheimschlüssel werden nur für ein einziges Gerät/Token Paar verwendet bzw. für jedes Paar wird ein neuer Schlüssel erzeugt.

Die Erzeugung neuer Tokens verlangt kein Umkopieren von Geheimschlüsseln, welche für andere Tokens verwendet werden (Sicherheitsrisiko).

Das Verfahren ist sehr einfach und kann deshalb auch in einer einfachen Zutrittskontrollsystemkonfiguration Gerät mit schlossartigem Geräteteil S - Token T effizient durchgeführt werden.

Patentansprüche

1. Zutrittskontrollverfahren für Geräte, welche erst nach Identifikation des Benutzers die Durchführung gewisser geschützter Operationen, bzw. den Zutritt zu geschützten Dateien ermöglichen, wobei ein

Token (T) genannter elektronischer Schlüssel mit einem als elektronisches Schloss fungierenden Teil (S) eines Gerätes, insbesondere einer datenverschlüsselnden Einrichtung, über Interfaces (6,7) ange-
dockt wird, ein erster Chiffrierschlüssel erzeugt wird und auf Speicherplätzen in Speichereinheiten (2,
8) des Geräteteils (S) und des Tokens (T) abgelegt wird, dadurch gekennzeichnet, dass zur Erzeugung
5 eines weiteren Chiffrierschlüssels für ein zweites Token (T) das Gerät erst nach Identifikation des Be-
nützers mit dem ersten erzeugten Token (T) in den schlüsselerzeugenden Modus übergeführt werden
kann, wonach für die neue Konfiguration Gerät – neues Token ein neuer Chiffrierschlüssel erzeugt
wird, welcher Schlüssel danach auf den nächsten freien Speicherplatz des Speicherblockes (2) des Ge-
räteteils (S) sowie auf den korrespondierenden Speicherplatz (21) im Speicherblock (8) des Tokens (T)
10 abgespeichert wird, dass dieser Vorgang bis zu einer systemimmanenten Maximalzahl von numerierten
Schlüsseln wiederholt werden kann, dass bei der Identifikation des Benützers die Speicherblöcke (2,8)
im Geräteteil (S) und im Token (T) nach übereinstimmenden Chiffrierschlüsseln abgesucht werden und
nach Auffinden eines entsprechenden Schlüssels einem Vergleichsblock (5) zugeführt werden, welcher
entscheidet, ob dem Benutzer zum angestrebten Betriebsmodus Zutritt zu gewähren ist.

2. Vorrichtung zur Durchführung des Verfahrens nach Patentanspruch 1, welche einen Geräteteil (S)
umfasst, welcher unter anderem ein elektronisches Schloss bildet und ein Token (T), welches als elektro-
nischer Schlüssel ausgebildet ist, welche beide (S, T) über Interfaces (6, 7) kommunizieren, dadurch ge-
kennzeichnet, dass das Token (T) eine zur Speicherung von mehreren Chiffrierschlüsseln ausgebildete
Speichereinheit (8) aufweist und dass der Geräteteil (S) eine dazu korrespondierende, für die Speiche-
20 rung mehrerer Chiffrierschlüssel ausgebildete Speichereinheit (2) und Such- und Vergleichseinrichtun-
gen (5) zum Auffinden von Speicherinhalten im Token (T), welche mit einem der Speicherinhalte im Gerä-
te teil (S) übereinstimmen, aufweist.

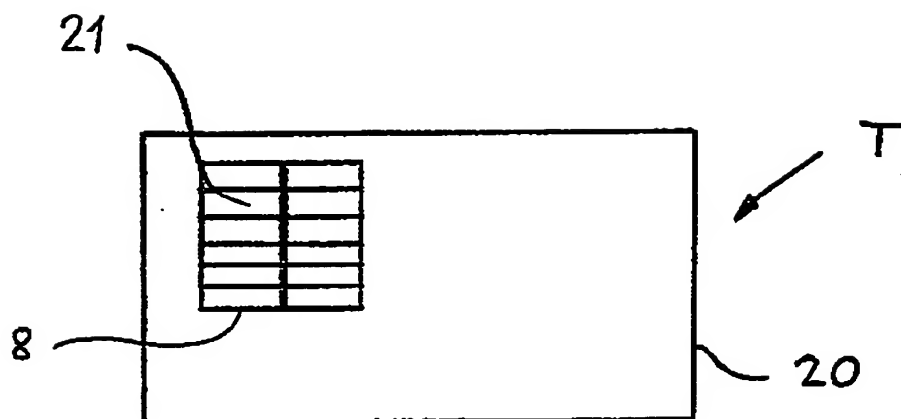


Fig. 1

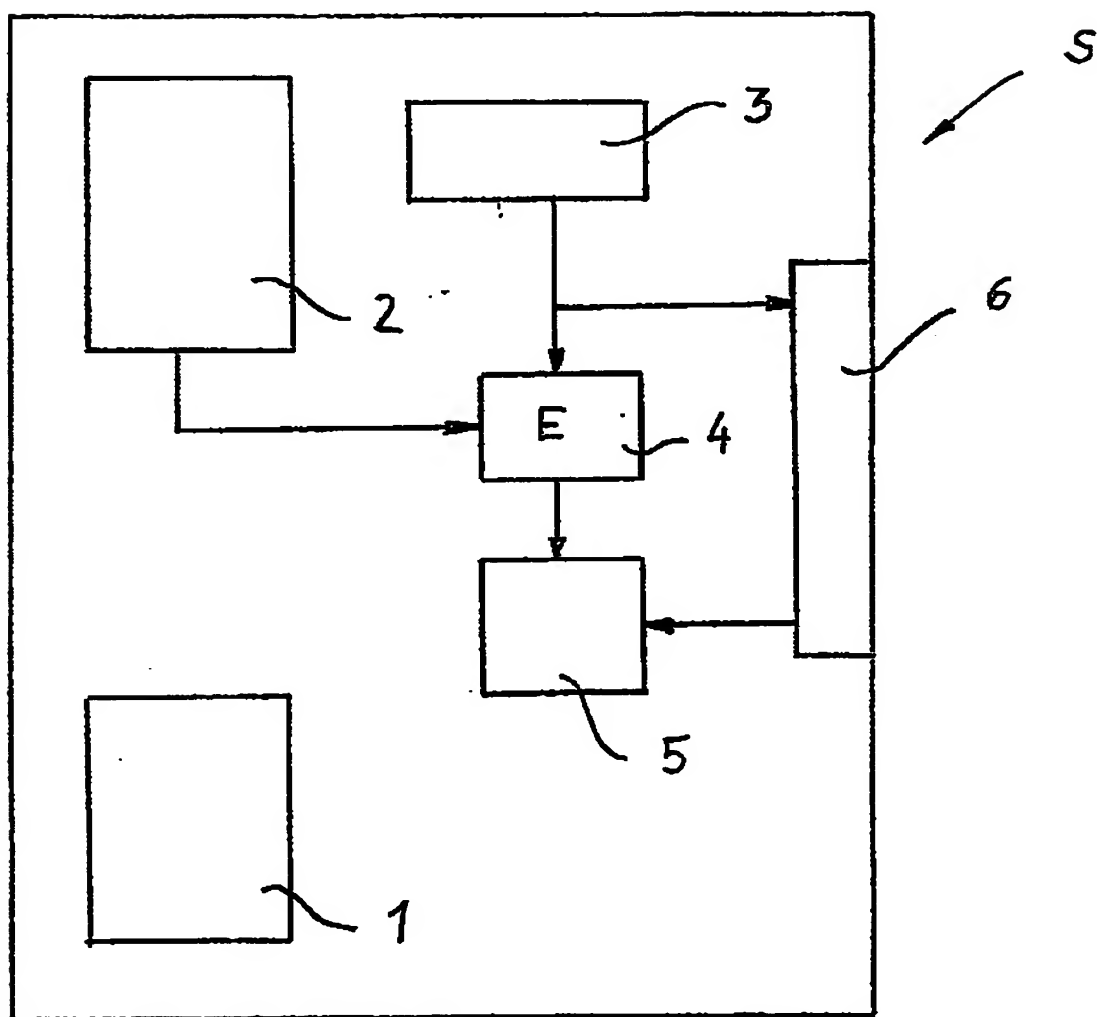


Fig. 2

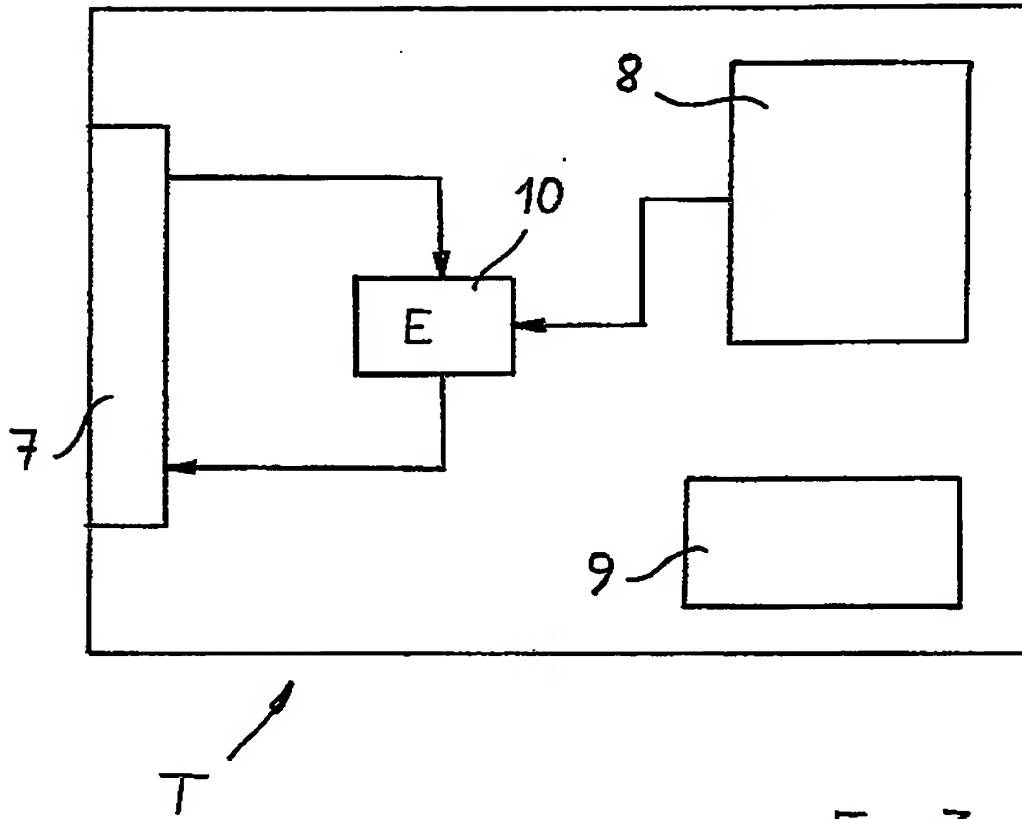


Fig. 3